

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
One Cellular Phone, belonging to Scott
Anderson, phone number (206) 794-9125,
located in Seattle, Washington

Case No. MJ20-247

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

One Cellular Phone, belonging to Scott Anderson, phone number (206) 794-9125, located in Seattle, Washington

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment A, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 1341 and 2
18 U.S.C. §§ 1343 and 2

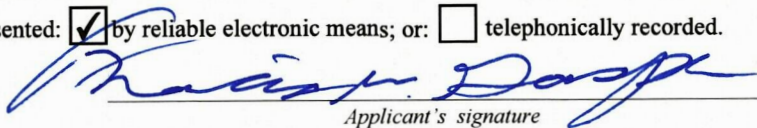
Offense Description
Mail Fraud
Wire Fraud

The application is based on these facts:

- ☒ See attached affidavit of FBI Special Agent Francis W. Gasper

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

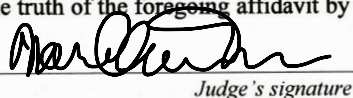
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Francis W. Gasper, FBI Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/14/2020


Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

1. I am a Special Agent for the Federal Bureau of Investigation (FBI). I have been a Special Agent for more than 24 years. I am currently assigned to the FBI Minneapolis Division, Bismarck, North Dakota office. I have participated in numerous investigations of alleged criminal activity. I assist other federal agencies' special agents and both state and local law enforcement when requested. Many of these crimes have involved the use of email or other forms of electronic communications. My duties include the investigation of financial crimes. I have primarily investigated financial crimes most of my career. I have attended a number of training courses relevant to financial crimes, including cybercrime and the review of evidence recovered from electronic storage devices such as computers and mobile telephones. Information contained in this affidavit is based upon personal knowledge arising from my participation in this investigation and upon information and belief. Sources of information include statements made to me by representatives of law enforcement agencies and other subjects/witnesses of the investigation. I have not included every fact known to me concerning this investigation.

3. Based on my training, experience, and the facts set forth in this affidavit, I believe there is probable cause to believe that violations of Title 18 U.S.C. §§ 1341, 1343,

1 and 2 have been committed by Scott Anderson and others. Additionally, I believe there is
2 probable cause to search the cellular telephone belonging to Anderson with the telephone
3 number (206) 794-9125, located in Seattle, Washington, for evidence of these crimes, fruits
4 of these crimes, and property used in committing these crimes, further described in
5 Attachment A. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I am
6 requesting a search warrant for the aforementioned telephone.

7 I. FACTS

8 4. On March 31, 2020, P.W., the owner of a small law firm located in Bismarck,
9 North Dakota, received an email from an individual using the name Anthonio Gaglio. In this
10 email, the person purporting to be Gaglio claimed to represent a construction company,
11 Viking Construction, Inc. (hereafter, Viking), with a Bridgeport, Connecticut, address.
12 According to the person claiming to be Gaglio, Viking was looking to sell a piece of
13 construction equipment to Magnum Contracting, which is located in Fargo, North Dakota.
14 The person claiming to be Gaglio asked P.W. to represent Viking in the transaction, since the
15 buyer supposedly wanted North Dakota law to cover the sale, and asked P.W. to create the
16 sales agreement. The person purporting to be Gaglio sent this email, and all future emails
17 described below, to P.W. from the email address anthonygagliosrr@gmail.com. I have
18 contacted Viking, which has informed me that this email address is not associated with
19 Viking and that Viking neither retained P.W. to represent it in any legal matters nor sent
20 P.W. any emails. As a result, I believe that the person claiming to be Gaglio sent emails in
21 interstate or foreign commerce, as part of a scheme described below to defraud P.W. and
22 obtain P.W.'s money by false and fraudulent pretenses and representations.

23 5. On April 10, 2020, P.W. received another email from the person claiming to be
24 Gaglio. In this email, the person claiming to be Gaglio informed P.W. that the construction
25 equipment buyer had sent P.W. a check and inquired as to whether P.W. had received the
26 check. Later that same day, the person claiming to be Gaglio sent P.W. a follow-up email
27 which listed a Federal Express tracking number and indicated P.W. had signed for the
28 package earlier that day.

1 6. P.W. in fact received the Federal Express package the person claiming to be
2 Gaglio had described. The package contained a Citibank cashier's check payable to P.W.'s
3 law firm in the amount of \$235,562.10. As directed in an email from the person claiming to
4 be Gaglio, P.W. deposited this cashier's check into the law firm's BNC National Bank
5 account, located in Bismarck, North Dakota, and sent an email to the person claiming to be
6 Gaglio at anthonygagliosrr@gmail.com containing an image of both the check and the
7 deposit slip. Therefore, I believe that, as part of the scheme to defraud P.W., the person
8 claiming to be Gaglio deposited or caused to be deposited a package to be sent or delivered
9 by a private or commercial interstate carrier to P.W., namely, the Federal Express package
10 containing the Citibank cashier's check.

11 7. On April 13, 2020, after P.W. had deposited the cashier's check, the person
12 purporting to be Gaglio sent P.W. an email instructing P.W. to send three wire transfers,
13 totaling \$185,000, to three different individuals or entities. These three individuals or
14 entities used different banks and were located in different states. As directed by the person
15 claiming to be Gaglio, P.W. had the law firm's bank send the wire transfers to these three
16 individuals or entities.

17 a. P.W. sent a wire transfer in the amount of \$60,000 to Doreese
18 Coles for "final inspection." This wire transfer was sent to Coles' Woodforest Bank
19 account, number *****4554.

20 b. P.W. sent a wire transfer in the amount of \$60,000 to Krystal
21 Fashion Corporation for "the service parts of the equipment." This wire transfer was
22 sent to Krystal Fashion Corporation's JP Morgan Chase bank account, number
23 *****1327.

24 c. P.W. sent a wire transfer in the amount of \$65,000 to Scott
25 Anderson "for the shipping of equipment." This wire transfer was sent to Anderson's
26 Citibank account, number ****0903.

27 8. Also on April 13, 2020, the person claiming to be Gaglio sent P.W. emails
28 requesting that P.W. forward to Gaglio the wire transfer confirmations. P.W. forwarded the

1 reference number information, but the person purporting to be Gaglio insisted P.W. send the
2 confirmation information for the wire transfers. As a result, P.W. emailed the person
3 claiming to be Gaglio three files containing images of the completed wires.

4 9. On April 16, 2020, BNC National Bank contacted P.W. and informed P.W.
5 that the \$235,562.10 Citibank cashier's check that P.W. had deposited into his law firm's
6 account was fraudulent. P.W. then contacted the FBI and also reported the fraud to the
7 Bismarck Police Department. P.W., working with BNC National Bank, also has contacted
8 the three banks where the wires were sent in an attempt to recover the funds.

9 10. On April 17, 2020, the person claiming to be Gaglio sent an email to P.W.
10 requesting that the remaining funds from the deposited cashier's check, minus P.W.'s fee, be
11 wired to a fourth different individual, in a fourth different location and utilizing a fourth
12 different bank. P.W. responded to the email requesting that Gaglio provide P.W. with a
13 telephone number so that P.W. could speak with Gaglio. The person claiming to be Gaglio
14 emailed P.W. a telephone number. P.W. attempted to call this number, but found that the
15 number was not a working number.

16 11. On April 20, 2020, a Citibank representative informed me that Anderson had
17 received the \$65,000 wire transfer from P.W. The representative told me that, after receiving
18 the money, Anderson transferred approximately \$5,000 to Coinbase to purchase Bitcoin. In
19 addition, Anderson transferred \$2,409.89 to Cash App and \$4,427.59 to MoonPay.
20 Anderson also made two ATM cash withdrawals totaling \$1,400. These cash withdrawals
21 were made ten minutes apart at two different Seattle, Washington, ATM locations; one
22 withdrawal for \$1,000 was made at a Chase Bank location and the other withdrawal was
23 made at an ATM located inside a Safeway.

24 12. I obtained images from Chase Bank and Safeway for these transactions. These
25 images show that the same individual, wearing a COVID-19 mask, conducted both
26 transactions. I also obtained Anderson's Washington State driver's license image. The
27 individual pictured conducting both of these ATM transactions appears to match Anderson's
28 driver's license image.

1 13. On April 21, 2020, I called Anderson, who lives in the Seattle, Washington, at
2 the cell number Anderson listed on his Citibank account, (206) 794-9125. During an initial
3 conversation, Anderson told me that the wire transfer he had received from P.W.'s law firm
4 was part of a legal settlement for a lawsuit involving a woman, Krista Medina, which was
5 filed in criminal court in King County, Washington. Anderson then ended the conversation
6 and requested that I contact him the next morning.

7 14. At approximately 9:15 p.m. on April 21, 2020, I received two telephone calls
8 on my FBI cell phone. The number displayed on these calls indicated the calls originated in
9 the United Kingdom. The caller spoke English very poorly with a heavy accent, which
10 sounded to me as if the caller might originally be from Africa. At approximately 2:40 a.m.
11 on April 22, 2020, I received two additional telephone calls, also on my cell phone. These
12 calls appeared to have been made with a VOIP using an area code associated with Northern
13 Iowa. This caller also spoke English with an accent and asked to speak with "Gasper." In
14 the background, I heard what sounded like a young child interacting with the caller. During
15 subsequent conversations, Anderson acknowledged to me that he had provided my contact
16 information to the individuals who had arranged the \$65,000 wire transfer sent to Anderson's
17 account. Anderson also sent me an email containing a screen shot of Anderson's telephone,
18 which contained a screen shot of an email I had sent to Anderson after our initial telephone
19 conversation containing my contact information.

20 15. Later on April 22, 2020, I called Anderson, as requested, at Anderson's
21 cellphone number; (206) 794-9125. During this second telephone conversation, Anderson
22 acknowledged that he had lied to me about the source of the money. During this
23 conversation, Anderson stated that his girlfriend's friend, Medina, had asked Anderson to
24 receive the \$65,000 for her. Anderson stated that he agreed to receive the wire transfer in
25 exchange for \$10,000. Anderson also acknowledged that he previously had received money
26 for Medina. Anderson stated that, on one of these occasions, he deposited a check from a
27 closed account into his then Wells Fargo account and received two Zelle payments that were
28 not authorized by the payor. Anderson said that, as a result of his actions, Wells Fargo

1 closed his account. Anderson also acknowledged that Key Bank and Umpqua had closed
2 bank accounts belonging to Anderson due to fraudulent deposits made into the accounts.
3 Anderson told me that the person who made these deposits had been arrested by British
4 authorities for fraud.

5 16. Anderson told me that, after receiving the \$65,000 wire transfer, he had
6 purchased Bitcoin and made the ATM withdrawals. Anderson sent me a chart that he had
7 prepared showing what Anderson did with the \$65,000 wired by P.W. This chart shows that
8 Anderson's share of the \$65,000 was supposed to be \$12,500.

9 17. My review of Wells Fargo bank records reveals that Anderson opened a bank
10 account on September 16, 2019. On November 11, 2019, Anderson deposited a Delta
11 Community Credit Union check from the account of C.G. On October 16, 2019, Wells
12 Fargo learned that C.G.'s account was closed and the check was no good. Additionally, the
13 records show that Anderson received two Zelle transfers deposited into the account from
14 S.W., on November 7, 2019, and C.R., on November 12, 2019. Wells Fargo later was
15 informed by S.W.'s and C.R.'s financial institutions that these transfers were made without
16 S.W.'s and C.R.'s permission. When interviewed by Wells Fargo, Anderson said that the
17 transfers were done so Anderson could purchase fabrics for S.W. and C.R. Wells Fargo
18 concluded Anderson was being evasive and closed Anderson's accounts.

19 18. My review of KeyBank reveals that Anderson opened his KeyBank account on
20 October 20, 2018. The records show deposits being made into Anderson's account by J.M.
21 When KeyBank branch employees spoke with J.M. concerning the deposits, J.M. stated that
22 he had met Anderson online and that the deposits were to repay a loan. The KeyBank
23 employee who spoke with J.M. indicated that J.M. seemed extremely nervous. The records
24 show that, between March 22, 2019, and July 23, 2019, Anderson sent nine wire transfers to
25 Nigeria. Anderson initially told KeyBank employees that the wire transfers were intended
26 for his girlfriend to purchase fabrics, but, when questioned further, Anderson said the wire
27 transfers were to pay for an apartment in the United Kingdom. Later, Anderson claimed the
28 funds were to pay for an attorney for his girlfriend.

1 19. My review of Umpqua Bank records shows that Anderson opened a bank
2 account online on November 22, 2019. Anderson received an ACH transaction, on March
3 19, 2020, for \$2,400, which the sending bank later informed Umpqua had not been
4 authorized by the sending account holder. On March 26, 2020, Anderson received an ACH
5 transaction for \$2,417 from Axos Bank, which later told Umpqua that there were insufficient
6 funds in the sender's account. Anderson withdrew half of the funds before Umpqua learned
7 of the problems, leaving Umpqua with a loss of \$2,350.70. Anderson failed to contact
8 Umpqua to discuss this account activity. As a result, Umpqua closed Anderson's account on
9 April 9, 2020. Umpqua's records show Anderson used the same cellphone number, (206)
10 794-9125, that I am seeking to search.

11 20. I have reviewed Woodforest National Bank records relating to Doreese Renee
12 Coles, who lives in the Commonwealth of Virginia. Those records reveal that Coles'
13 account was opened on November 2, 2019. On April 13, 2020, Coles received a \$60,000
14 wire transfer from P.W.'s law firm. At the time the wire transfer was received, Coles had a
15 balance of \$225.86. On April 14, 2020, Coles withdrew \$5,000 in cash from her account.
16 On April 15, 2020, Coles made purchases and paid bills amounting to more than \$750. The
17 same day, Coles made two transfers to a Cash App account in the name of "Reesey" totaling
18 \$2,650. Coles also made a \$900 deposit to a Wave account. On April 16, 2020, Coles again
19 withdrew \$5,000 in cash from her account. Coles also made another transfer of \$4,845 to the
20 Cash App account in the name "Reesey" and a \$999 deposit to a Wave account.

21 21. I have reviewed video images Woodforest National Bank provided concerning
22 the \$5,000 cash withdrawals from Coles' account. I also obtained Coles' driver's license
23 photograph from the Commonwealth of Virginia. The images of the individual making the
24 two cash withdrawals appear to match Coles' driver's license photograph.

25 22. On April 23, 2020, I called Coles at the telephone number Coles listed on her
26 Woodforest National Bank account. During this initial conversation, Coles stated that the
27 \$60,000 wire transfer sent by P.W. was for a business Coles operated with a friend. Coles
28 stated that the money was for both personal and business transactions. Coles stated that she

1 had been working with a friend in Nigeria who was in the oil business. Coles acknowledged
2 she had taken \$5,000 out of her account in cash, on April 14, 2020, and April 16, 2020.
3 Coles stated that Woodforest National Bank told her she could only take \$5,000 in cash in a
4 one-day period. Coles stated she used the money to pay bills and gave some to her friends
5 and family. Coles stated that her Facebook identity was "Reeseey Reese." Coles said that she
6 was supposed to send the rest of the \$60,000 wire transfer money to her friend in Africa.

7 23. Coles eventually provided me the name and other information for two
8 individuals in Nigeria to whom Coles had sent money. Coles said she communicated with
9 these individuals using Facebook Messenger. When I asked who else was involved in the
10 wire transfer Coles received from P.W., Coles replied "Scott Anderson" and texted me a
11 picture of handwritten notes with Anderson's address and information relating to one of the
12 individuals in Nigeria with whom Coles was working. Coles also texted me a screenshot of
13 the wire information BNC National Bank provided P.W. concerning the \$65,000 wire
14 transfer P.W. sent to Anderson. I have reviewed emails P.W. sent to the person claiming to
15 be Gaglio which contained this same wire transfer screenshot. Coles also texted me a
16 screenshot of part of an email sent by BNC National Bank to P.W. that had the reference
17 numbers of the three wire transfers P.W. made to Coles, Anderson, and Krystal Fashion
18 Corporation, which P.W. had forwarded to the person claiming to be Gaglio.

19 24. Coles confirmed during telephone conversations with me that the \$60,000 wire
20 transfer was not the first money Coles had received on behalf of the two individuals with
21 whom Coles was working in Nigeria.

22 25. After initially speaking with me, Coles communicated with one of her contacts
23 in Nigeria, whom she referred to as Om. Coles told Om that the FBI had contracted Coles.
24 Om asked Coles what the FBI asked about, and also asked that Coles provide the name and
25 telephone number of the person from the FBI. Coles provided Om this information. Om
26 then told Coles that I was the same FBI Agent who had contacted Anderson. Coles told me
27 that Om was working with at least two additional people, other than Anderson, in the United
28 States and at least one other individual in Nigeria.

1 26. During telephone conversations with me, Anderson told me that Anderson
2 used his cellphone (206) 794-9125 in all his communications with Medina. Anderson told
3 me that he does not own a computer and uses his cellphone for all electronic
4 communications, including include email. Anderson sent me more than ten emails dated
5 between April 22, 2020, and April 30, 2020. Many of these emails contained attachments,
6 including screenshots of Anderson's Bitcoin transactions, Google Hangout conversations
7 with Medina, and Citibank records.

8 27. Based on my training and experience, I know that individuals, such as
9 Anderson, involved in financial crimes, such as mail fraud and wire fraud, often use portable
10 electronic devices such as cellphones to log on to financial accounts and email accounts.
11 Records of this activity often remain on these devices for a long period of time.

12 **II. CELLULAR TELEPHONES AND WIRELESS COMMUNICATION DEVICES**

13 28. Cellular telephones and other wireless communication devices such as tablets
14 (e.g. iPads and other similar devices) are used for voice and data communication through
15 cellular or Wi-Fi signals. These devices send signals through networks of
16 transmitter/receivers, enabling communication with other wireless devices or traditional
17 "land line" telephones. Many such devices can connect to the Internet and interconnect with
18 other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth or near
19 field communication (NFC). In addition to enabling voice communications, wireless
20 communication devices offer a broad range of capabilities. These capabilities include:
21 storing names and phone numbers in electronic "address books" or "contact lists;" sending,
22 receiving, and storing short message service (SMS) and multi-media messaging service
23 (MMS) messages, other text messages, and e-mail; taking, sending, receiving, and storing
24 still photographs and moving video; storing and playing back audio files; and storing dates,
25 appointments, and other information on personal calendars.

26 29. Based upon my training and experience, all of these types of information may
27 be evidence of crimes under investigation. Stored e-mails and text messages not only may
28 contain communications relating to crimes, but also help identify the participants in those

1 crimes. Address books and contact lists may help identify co-conspirators. Similarly,
2 photographs on a cellular telephone may help identify the device user and co-conspirators,
3 either through his or her own photographs, or through photographs of friends, family, and
4 associates. Digital photographs also often have embedded location data GPS information
5 that identifies where the photo was taken. This location information is helpful because, for
6 example, it can show where coconspirators meet, where they traveled, and where assets
7 might be located. Calendar data may reveal the timing and extent of criminal activity.

8 30. A cellphone used for cellular voice communication will also typically contain a
9 “call log” or “stored list of recent, received, sent or missed calls” which records the
10 telephone number, date, and time of calls made to and from the phone. The stored list of
11 recent received, missed, and sent calls is important evidence. It identifies telephones
12 recently in contact with the telephone user and may help identify co-conspirators, establish a
13 timeline of events and/or identify who was using the phone at any particular time.

14 31. In addition, wireless communication devices will typically have an assigned
15 number and identifying serial number such as an ESN, MIN, IMSI or IMEI number that
16 identifies the particular device on any network. This identifying information may also
17 include the device’s assigned name (as assigned by the user) and network addresses such as
18 assigned IP addresses and MAC address. I know based on my training and experience that
19 such information may be important evidence of who used a device, when it was used, and for
20 what purposes it may have been used. This information can be used to obtain toll records
21 and other subscriber records, to identify contacts by this telephone with other telephones, or
22 to identify other telephones used by the same subscriber or purchased as part of a package.

23 32. Many wireless communication devices including cellular telephones such as
24 iPhones, iPads, Android phones, and other “smart phones” as well as tablet devices such as
25 Apple iPads may also be used to browse and search the Internet. These devices may browse
26 and search the internet using traditional web browsers such as Apple’s Safari browser or
27 Google’s Chrome browser as well as through third-party applications such as Facebook,
28 Twitter and others that also provide the ability to browse and search the internet. Based on

1 my training and experience, I know that internet browsing history may include valuable
2 evidence regarding the identity of the user of the device. This evidence may include online
3 user names, account numbers, e-mail accounts and bank accounts as well as other online
4 services. Internet browsing history may also reveal important evidence about a person's
5 location and search history. Search history is often valuable evidence that may help reveal a
6 suspect's intent and plans to commit a crime or efforts to hide evidence of a crime and may
7 also help reveal the identity of the person using the device.

8 33. Cellular telephones and other wireless communication devices are also capable
9 of operating a wide variety of communication applications or "apps" that allow a user to
10 communicate with other devices via a variety of communication channels. These additional
11 communication channels include traditional cellular networks, voice over internet protocol,
12 video conferencing (such as FaceTime and Skype), and a wide variety of messaging
13 applications (such as SnapChat, WhatsApp, Signal, Telegram, Viber and iMessage). I know
14 based on my training and experience that there are hundreds of different messaging and
15 conferencing applications available for popular cellular telephones and that the capabilities
16 of these applications vary widely for each application. Some applications include end-to-end
17 encryption that may prevent law enforcement from deciphering the communications without
18 access to the device and the ability to "unlock" the device through discovery of the user's
19 password or other authentication key.

20 34. Other applications facilitate multiple forms of communication including text,
21 voice, and video conferencing. Information from these communication apps may constitute
22 evidence of the crimes under investigation to the extent they may reveal communications
23 related to the crime or evidence of who the user of the device was communicating with and
24 when those communications occurred. Information from these communication apps may
25 also reveal alias names used by the device owner that may lead to other evidence.

26 35. I know based on my training and experience that obtaining a list of all the
27 applications present on a cellphone may provide valuable leads in an investigation. By
28 determining what applications are present on a device, an investigator may conduct follow-

1 up investigation, including obtaining subscriber records and logs to determine whether the
2 device owner or operator has used each particular messaging application. This information
3 may be used to support additional search warrants or other legal process to capture those
4 communications and discover valuable evidence.

5 36. Cellphones and other wireless communication devices may also contain
6 geolocation information indicating where the device was at particular times. Many of these
7 devices track and store GPS and cell-site location data to provide enhanced location based
8 services, serve location-targeted advertising, search results, and other content. Numerous
9 applications available for wireless communication devices collect and store location data.
10 For example, when location services are enabled on a handheld mobile device, many photo
11 applications will embed location data with each photograph taken and stored on the device.
12 Mapping applications such as Google Maps may store location data including lists of
13 locations the user has entered into the application. Location information may constitute
14 evidence of the crimes under investigation because that information may reveal whether a
15 suspect was at or near the scene of a crime at any given moment and may also reveal
16 evidence related to the identity of the user of the device.

17 37. Searching a cellular phone or wireless communication device is frequently
18 different than conducting a search of a traditional computer. Agents and forensic examiners
19 will attempt to extract the contents of the cellular phone or wireless communication device
20 using a variety of techniques designed to accurately capture the data in a forensically sound
21 manner in order to make the data available to search for the items authorized by the search
22 warrant. This may involve extracting a bit-for-bit copy of the contents of the device or, if
23 such an extraction is not feasible for any particular device, the search may involve other
24 methods of extracting data from the device such as copying the device's active user files
25 (known as a logical acquisition) or copying the device's entire file system (known as a file
26 system acquisition). If none of these methods are supported by the combination of tools
27 available to the examiner and the device to be searched, the agents and examiners may
28

1 conduct a manual search of the device by scrolling through the contents of the device and
2 photographing the results.

3 **III. CONCLUSION**

4 38. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I submit that
5 there is probable cause that evidence and fruits of, and property used in committing, the
6 crimes of mail fraud, in violation of Title 18, United States Code, Sections 1341 and 2, and
7 wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2, that is, the
8 items listed in Attachment A, attached hereto, will be found on Scott Anderson's mobile
9 telephone.

10 

11 FRANCIS W. GASPER
12 Special Agent
13 Federal Bureau of Investigation

14
15 The above-named agent provided a sworn statement attesting to the truth of the
16 foregoing affidavit on 14th day of May, 2020.

17 

18 MARY ALICE THEILER
19 United States Magistrate Judge

ATTACHMENT A

1. All records on the cell phone belonging to Scott Anderson, with the telephone number (206) 794-9125, that relate to violations of: 1) mail fraud, in violation of Title 18, United States Code, Sections 1341 and 2; and 2) wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2 for the period from November 1, 2018 to the present, including:

- a. all e-mails, text messages, chats (including communications in any messaging or other apps), or other records relating to Viking Construction, Inc., Magnum Contracting, or Krystal National Fashion Corporation;
- b. all e-mails, text messages, chats, or other communications (including communications in any messaging or other apps) with, or records relating to, any of Anthony or Anthonio Gaglio, Krista Medina, Doreese Coles, or FNU Om;
- c. all records relating to the purchase of fabrics or the oil business
- d. all records relating to any transfer of money from BNC National Bank, or to the subsequent disposition of that money;
- e. all records relating to any bank account at Citibank, Wells Fargo Bank, Umpqua Bank, KeyBank, or Woodforest Bank
- f. all records relating to any investigation by law enforcement, including the FBI, or by any bank;
- g. all Identification documents, including forged identification documents, of any person other than Scott Anderson;
- h. all call history and call logs;
- i. all contracts/address books;
- j. all internet or browsing history;
- k. any calendar information or other information of Anderson's schedule or travel;
- l. all historical location/GPS information;

- 1 m. all photographs, video recordings, or audio recordings relating to the items
- 2 described in a) through f) above;
- 3 n. all bank records, checks, credit card bills, account information, and other
- 4 financial records;
- 5 o. all records of transactions involving cryptocurrency, including Bitcoin;
- 6 2. Evidence of user attribution showing who used or owned the telephone at the
- 7 time the crimes described in this warrant were committed;
- 8 3. Records evidencing the use of the Internet Protocol addresses to communicate
- 9 with Google and other mail servers including:
- 10 a. records of Internet Protocol addresses used;
- 11 b. records of Internet activity, including firewall logs, caches, browser history and
- 12 cookies, “bookmarked” or “favorite” web pages, search terms that the user
- 13 entered into any Internet search engine, and records of user-typed web
- 14 addresses.

15 As used above, the terms “records” and “information” include all of the foregoing
16 items of evidence in whatever form and by whatever means they may have been created or
17 stored.

18 This warrant authorizes a search of the person of Scott Anderson if necessary to, and
19 for the limited purpose of seizing the cellular telephone described in this warrant.

20 This warrant authorizes a review of electronic storage media and electronically stored
21 information seized or copied pursuant to this warrant in order to locate evidence, fruits, and
22 instrumentalities described in this warrant. The review of this electronic data may be
23 conducted by any government personnel assisting in the investigation, who may include, in
24 addition to law enforcement officers and agents, attorneys for the government, attorney
25 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete
26 copy of the seized or copied electronic data to the custody and control of attorneys for the
27 government and their support staff for their independent review.